

(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関  
国際事務局



(43) 国際公開日  
2001 年 7 月 19 日 (19.07.2001)

PCT

(10) 国際公開番号  
WO 01/52474 A1

(51) 国際特許分類<sup>7</sup>: H04L 9/32, 9/08, G06F 17/60

(21) 国際出願番号: PCT/JP01/00159

(22) 国際出願日: 2001 年 1 月 12 日 (12.01.2001)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:  
特願2000-006989 2000 年 1 月 14 日 (14.01.2000) JP  
特願2000-041317 2000 年 2 月 18 日 (18.02.2000) JP

(71) 出願人 (米国を除く全ての指定国について): 松下電  
器産業株式会社 (MATSUSHITA ELECTRIC INDUS-  
TRIAL CO., LTD.) [JP/JP]; 〒571-8501 大阪府門真市  
大字門真1006番地 Osaka (JP).

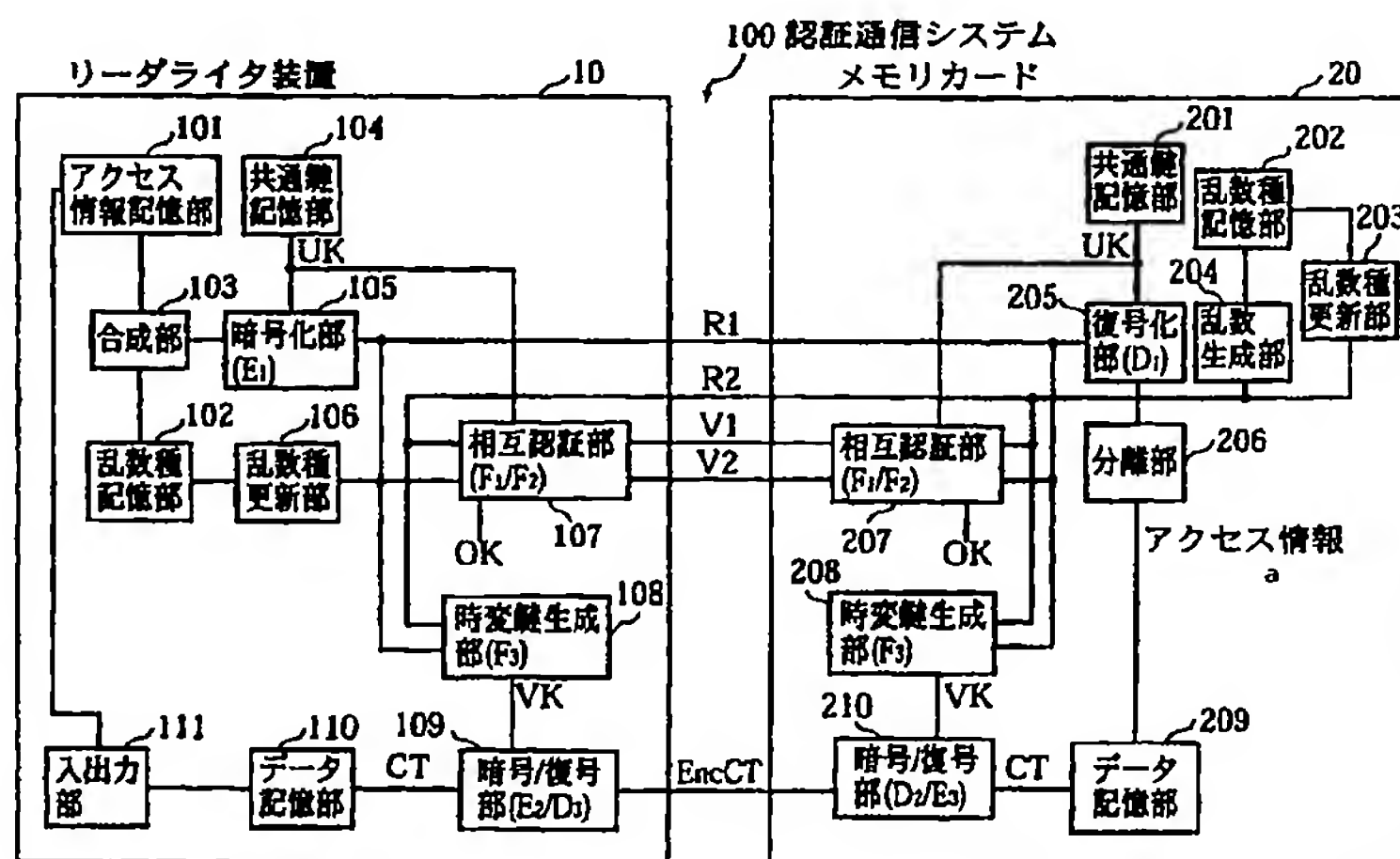
(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 柴田 修  
(SHIBATA, Osamu) [JP/JP]; 〒570-0032 大阪府守口  
市菊水通1-16-22 Osaka (JP). 湯川泰平 (YUGAWA,  
Taihei) [JP/JP]; 〒631-0041 奈良県奈良市学園大和町  
6-708-1-513 Nara (JP). 関部 勉 (SEKIBE, Tsutomu)  
[JP/JP]; 〒573-0047 大阪府枚方市山之上5-49-34 Osaka  
(JP). 廣田照人 (HIROTA, Teruto) [JP/JP]; 〒570-0015  
大阪府守口市梶町1-20-1-306 Osaka (JP). 齋藤義行  
(SAITO, Yoshiyuki) [JP/JP]; 〒576-0053 大阪府交野市  
郡津1-1-611 Osaka (JP). 大竹俊彦 (OTAKE, Toshihiko)

[続葉有]

(54) Title: AUTHENTICATION COMMUNICATION DEVICE AND AUTHENTICATION COMMUNICATION SYSTEM

(54) 発明の名称: 認証通信装置及び認証通信システム



10...READER/WRITER  
101...ACCESS INFORMATION STORAGE SECTION  
104...COMMON KEY STORAGE SECTION  
103...SYNTHESIZING SECTION  
105...ENCRYPTING SECTION  
102...RANDOM NUMBER TYPE STORAGE SECTION  
106...RANDOM NUMBER TYPE UPDATING SECTION  
107...MUTUAL AUTHENTICATING SECTION  
108...TIME-VARYING KEY GENERATING SECTION  
111...I/O SECTION  
110...DATA STORAGE SECTION  
109...ENCRYPTING/DECRYPTING SECTION  
100...AUTHENTICATION COMMUNICATION SYSTEM  
20...MEMORY CARD

201...COMMON KEY STORAGE SECTION  
202...RANDOM NUMBER TYPE STORAGE SECTION  
203...RANDOM NUMBER TYPE UPDATING SECTION  
205...DECRYPTING SECTION  
204...RANDOM NUMBER GENERATING SECTION  
207...MUTUAL AUTHENTICATING SECTION  
206...SEPARATING SECTION  
208...TIME-VARYING KEY GENERATING SECTION  
210...ENCRYPTING/DECRYPTING SECTION  
209...DATA STORAGE SECTION  
a...ACCESS INFORMATION

(57) Abstract: An authentication communication device comprises a storage medium having an area for storing digital information therein and an access unit for reading digital information from the area and writing digital information in the area. The access unit authenticates the storage medium according to a challenge response authentication protocol using disturbed access information produced by disturbing access information indicative of the area. The access unit is authenticated by the storage medium. When the validity is of both the storage medium and the access unit authenticated, the access unit reads out digital information from the area of the storage medium corresponding to access information separated from the disturbed access information or writes digital information therein.

[続葉有]



[JP/JP]; 〒662-0095 兵庫県西宮市美作町5-12 Hyogo (JP).

(74) 代理人: 中島司朗(NAKAJIMA, Shiro); 〒531-0072 大阪府大阪市北区豊崎三丁目2番1号 淀川5番館6F Osaka (JP).

(81) 指定国 (国内): AU, CN, ID, KR, MX, US.

(84) 指定国 (広域): ヨーロッパ特許 (DE, FR, GB, NL).

添付公開書類:  
— 国際調査報告書

2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(57) 要約:

デジタル情報を記憶する領域を有する記憶媒体と、前記領域からデジタル情報を読み出し、又は前記領域へデジタル情報を書き込むアクセス装置とから構成され、前記アクセス装置において前記領域を示すアクセス情報を攪乱した攪乱化アクセス情報を用いたチャレンジレスポンス型認証プロトコルにより前記記憶媒体の認証を行うと共に、前記記憶媒体において、前記アクセス装置の認証を行い、共に正当性が認証された場合には、前記アクセス装置によって前記攪乱化アクセス情報から分離されたアクセス情報に応じた前記記憶媒体の前記領域にデジタル情報を読み出し、又は前記領域に書き込む。

## 明 細 書

## 認証通信装置及び認証通信システム

## 5 技術分野

本発明は、デジタル著作物を機器と記録媒体との間で転送する場合において、機器と記録媒体との間で、相互に正当性を認証する技術に関する。

## 10 背景技術

近年、デジタル情報圧縮技術の進展と、インターネットに代表されるグローバルな通信インフラの爆発的な普及によって、音楽、画像、映像、ゲームなどの著作物をデジタル著作物として通信回線を介して各家庭に配信することが実現されている。

- 15 デジタル著作物の著作権者の権利や、流通業者の利益を保護するための流通配信システムを確立するために、通信の傍受、盗聴、なりすましなどによる著作物の不正な入手や、受信したデータを記録している記録媒体からの違法な複製、違法な改竄などの不正行為を防止することが課題となっており、正規のシステムかどうかの判別を行ったり、データス
- 20 クランブルを行う暗号及び認証などの著作物保護技術が必要とされている。

- 著作物保護技術については、従来より様々なものが知られており、代表的なものとして、著作物の保護を要する機密データが格納されている機密データ記憶領域にアクセスする際に、機器間で乱数と応答値の交換
- 25 を行って、相互に正当性を認証しあい、正当である場合のみ、アクセスを許可するチャレンジレスポンス型の相互認証技術がある。

しかしながら、例えば、相互認証を正規な機器を用いて行った後に、正当機器になりすまして、機密データ記憶領域にアクセスすることによ

り、機密データを不正に入手する行為が考えられる。

#### 発明の開示

そこで本発明はかかる問題点に鑑みてなされたものであり、機密データ記憶領域にアクセスするための情報が漏洩されないアクセス装置、記録媒体、認証通信システム、認証通信方法及び認証通信プログラムを記録している記録媒体を提供することを目的とする。

上記目的を達成するために本発明は、デジタル情報を記憶する領域を有する記録媒体と、前記領域からデジタル情報を読み出し又は前記領域へデジタル情報を書き込むアクセス装置とから構成される認証通信システムであって、前記アクセス装置から前記記録媒体へ、前記領域を示すアクセス情報を攪乱して生成した攪乱化アクセス情報を伝送することにより、前記アクセス装置がチャレンジレスポンス型の認証プロトコルによる前記記録媒体の正当性の認証を行う第1認証フェーズと、前記記録媒体が前記アクセス装置の正当性の認証を行う第2認証フェーズと、前記記録媒体と前記アクセス装置とがともに正当性を有すると認証された場合に、前記記録媒体は、伝送された攪乱化アクセス情報からアクセス情報を抽出し、前記アクセス装置は、抽出された前記アクセス情報により示される領域からデジタル情報を読み出し、又は前記アクセス情報により示される領域へデジタル情報を書き込む転送フェーズとを含むことを特徴とする。

これによって、相互認証と同時に、機密のデータを記録している機密データ記憶領域にアクセスするための情報を攪乱して転送するので、機密データ記憶領域にアクセスするための情報の機密性を高めることができる。

また、仮に、機密データ記憶領域にアクセスするための情報が、不正ななりすましにより、別の情報に改竄されて転送された場合であっても、相互認証が成功しないので、機密データ記憶領域にアクセスできないようにすることができる。

## 図面の簡単な説明

図 1 は、認証通信システム 100 の具体的な構成例としての認証通信システム 30 及び 31 の外観を示す。図 1 (a) は、パーソナルコンピュータとメモリカード 20 から構成される認証通信システム 30 の外観を示し、図 1 (b) は、ヘッドホンステレオ、メモリカード 20 及びヘッドホンから構成される認証通信システム 31 の外観を示す。

図 2 は、認証通信システム 100 を構成するリーダライタ装置 10 及びメモリカード 20 のそれぞれ構成を示すブロック図である。

図 3 は、アクセス情報、乱数種及び乱数化アクセス情報のデータ構造を示す。図 4 は、認証通信システム 100 の動作を示すフローチャートであり、特に、メモリカードに記憶されている情報を読み出す場合を想定したものである。図 5 に続く。

図 5 は、認証通信システム 100 の動作を示すフローチャートである。図 4 から続く。

図 6 は、認証通信システム 100 の動作を示すフローチャートであり、特に、リーダライタ装置 10 は、メモリカードに情報を書き込む装置であると想定した場合のものである。

図 7 は、別の実施の形態としての、認証通信システム 100 a の構成を示すブロック図である。

図 8 は、認証通信システム 100 a に固有の動作を示すフローチャートである。

図 9 は、別の実施の形態としての、認証通信システム 100 b の構成を示すブロック図である。

図 10 は、認証通信システム 100 b に固有の動作を示すフローチャートである。

## 発明を実施するための最良の形態

本発明に係る一つの実施の形態としての認証通信システム 100 について説明する。

## 1. 認証通信システム 100 の外観と利用形態

認証通信システム 100 の具体的な構成例としての認証通信システム 30 及び 31 の外観図を図 1 (a) 及び (b) に示す。

図 1 (a) に示すように、認証通信システム 30 は、パーソナルコンピュータとメモリカード 20 から構成される。パーソナルコンピュータは、ディスプレイ部、キーボード、スピーカ、マイクロプロセッサ、RAM、ROM、ハードディスクユニットなどを備えており、通信回線を経由してインターネットに代表されるネットワークに接続されている。メモリカード 20 は、メモリカード挿入口から挿入され、パーソナルコンピュータに装着される。

図 1 (b) に示すように、認証通信システム 31 は、ヘッドホンステレオ、メモリカード 20 及びヘッドホンから構成される。メモリカード 20 は、ヘッドホンステレオのメモリカード挿入口から挿入されて、ヘッドホンステレオに装着される。ヘッドホンステレオは、上面に複数の操作ボタンが配置されており、別の側面にヘッドホンが接続されている。

利用者は、メモリカード 20 をパーソナルコンピュータに装着し、インターネットを経由して、外部の Web サーバ装置から音楽などのデジタル著作物を取り込み、取り込んだデジタル著作物をメモリカード 20 に書き込む。次に、利用者は、デジタル著作物の記録されているメモリカード 20 をヘッドホンステレオに装着し、メモリカード 20 に記録されているデジタル著作物をヘッドホンステレオにより再生して、楽しむ。

ここで、パーソナルコンピュータとメモリカード 20 との間において、また、ヘッドホンステレオとメモリカード 20 との間において、チャレンジレスポンス型の認証プロトコルによる各機器の正当性の認証を行い、相互に正当な機器であることが認証された場合にのみ、各機器間でデジタル著作物の転送が行われる。

## 2. 認証通信システム 100 の構成

認証通信システム 100 は、図 2 に示すように、リーダライタ装置 1



0 及びメモリカード 20 から構成される。ここで、リーダライタ装置 10 は、図 1 (a) 及び (b) に示すパーソナルコンピュータ及びヘッドホンステレオに相当する。

## 2. 1 リーダライタ装置 10 の構成

5 リーダライタ装置 10 は、アクセス情報記憶部 101、乱数種記憶部 102、合成部 103、共通鍵記憶部 104、暗号化部 105、乱数種更新部 106、相互認証部 107、時変鍵生成部 108、暗号復号部 109、データ記憶部 110 及び入出力部 111 から構成されている。

10 リーダライタ装置 10 は、具体的には、マイクロプロセッサ、RAM、ROMその他を備え、ROMなどにコンピュータプログラムが記録されており、マイクロプロセッサは、前記コンピュータプログラムに従って動作する。

### (1) 入出力部 111

15 入出力部 111 は、利用者の操作を受け付けて、メモリカード 20 のデータ記憶部 209 に記憶されている音楽情報にアクセスするためのアクセス情報を生成する。アクセス情報は、図 3 に示すように、32 ビット長であり、メモリカード 20 のデータ記憶部の領域のアドレスを示すアドレス情報と、前記領域のサイズを示すサイズ情報とから構成される。アドレス情報は、24 ビット長であり、サイズ情報は、8 ビット長である。

20 また、入出力部 111 は、データ記憶部 110 から音楽情報 CT を読み出し、読み出した音楽情報 CT を音声信号に変換して出力する。

25 また、入出力部 111 は、利用者の操作を受け付けて、外部から音楽情報 CT を取得し、取得した音楽情報 CT をデータ記憶部 110 へ書き込む。

### (2) アクセス情報記憶部 101

アクセス情報記憶部 101 は、具体的には、半導体メモリから構成され、アクセス情報を記憶する領域を備えている。

(3) 乱数種記憶部 1 0 2

乱数種記憶部 1 0 2 は、具体的には、半導体メモリから構成され、図 3 に示すような 6 4 ビット長の乱数種をあらかじめ記憶している。乱数種は、装置の製造時に記録される。

5 乱数種記憶部 1 0 2 は、外部から直接アクセスできる手段を有しておらず、プロテクトされている記憶手段である。

(4) 合成部 1 0 3

合成部 1 0 3 は、アクセス情報記憶部 1 0 1 からアクセス情報を読み出し、乱数種記憶部 1 0 2 から乱数種を読み出す。次に、図 3 に示すように、読み出した前記アクセス情報と、読み出した前記乱数種の下位 3 2 ビットとを結合して、6 4 ビット長の乱数化アクセス情報を生成する。生成した乱数化アクセス情報を暗号化部 1 0 5 へ出力する。

(5) 共通鍵記憶部 1 0 4

15 共通鍵記憶部 1 0 4 は、具体的には、半導体メモリから構成され、5 6 ビット長の共通鍵 UK を記憶する領域を備えている。リーダライタ装置 1 0 は、メモリカード 2 0 から共通鍵記憶部 2 0 1 に記憶されている共通鍵 UK を秘密に取得し、共通鍵記憶部 1 0 4 は、取得した共通鍵 UK を記憶する。

20 共通鍵記憶部 1 0 4 は、外部から直接アクセスできる手段を有しておらず、プロテクトされている記憶手段である。

(6) 暗号化部 1 0 5

25 暗号化部 1 0 5 は、共通鍵記憶部 1 0 4 から共通鍵 UK を読み出し、合成部 1 0 3 から乱数化アクセス情報を受け取る。次に、暗号化部 1 0 5 は、共通鍵 UK を用いて、受け取った乱数化アクセス情報に暗号アルゴリズム E 1 を施して暗号化アクセス情報 R 1 を生成する。ここで、暗号化部 1 0 5 は、暗号アルゴリズム E 1 として、DES (Data Encryption Standard) を用いる。

次に、暗号化部 1 0 5 は、生成した暗号化アクセス情報 R 1 を、相互



認証部 107 と、乱数種更新部 106 と、時変鍵生成部 108 とへ出力する。また、生成した暗号化アクセス情報 R1 を、メモリカード 20 の復号化部 205 と、相互認証部 207 と、時変鍵生成部 208 とへ出力する。

- 5       このようにして生成された暗号化アクセス情報 R1 は、アクセス情報に攪乱 (s c r a m b l e) 処理を施して得られる攪乱化情報である。

(7) 乱数種更新部 106

- 乱数種更新部 106 は、暗号化部 105 から暗号化アクセス情報 R1 を受け取り、受け取った暗号化アクセス情報 R1 を新たな乱数種として  
10 乱数種記憶部 102 へ上書きする。

(8) 相互認証部 107

相互認証部 107 は、暗号化アクセス情報 R1 を受け取り、共通鍵記憶部 104 から共通鍵 UK を読み出し、受け取った R1 と共通鍵 UK とを用いて、式 1 により、応答値 V2' を算出する。

- 15       (式 1)    $V2' = F1(R1, UK) = SHA(R1 + UK)$

ここで、関数 F1 (a、b) は、一例として、a と b とを結合し、その結合結果に対して SHA (S e c u r e   H a s h   A l g o r i t h m) を施す関数である。なお、+ は、結合を示す演算子である。

相互認証部 107 は、相互認証部 207 から応答値 V2 を受け取る。

- 20       次に、相互認証部 107 は、V2 と V2' とが一致するか否かを判断し、一致しない場合には、メモリカード 20 が不正な装置であると認定し、他の構成部に対して以降の動作の実行を禁止する。一致する場合には、相互認証部 107 は、メモリカード 20 が正当な装置であると認定し、他の構成部に対して以降の動作の実行を許可する。

- 25       また、相互認証部 107 は、乱数生成部 204 から乱数 R2 を受け取り、受け取った乱数 R2 と、前記共通鍵 UK とを用いて、式 2 により、応答値 V1 を算出し、算出した応答値 V1 を相互認証部 207 へ出力する。

$$(式2) \quad V1 = F2(R2, UK) = SHA(R2 + UK)$$

(9) 時変鍵生成部108

時変鍵生成部108は、メモリカード20が正当な装置であると認定され、動作の実行を許可される場合に、暗号化アクセス情報R1と乱数R2とを受け取り、R1とR2とから、式3を用いて時変鍵VKを生成する

$$(式3) \quad VK = F3(R1, R2) = SHA(R1 + R2)$$

次に、時変鍵生成部108は、生成した時変鍵VKを暗号復号部109へ出力する。

(10) 暗号復号部109

暗号復号部109は、時変鍵生成部108から時変鍵VKを受け取る。

暗号復号部109は、暗号復号部210から暗号化音楽情報EncCTを受け取り、前記時変鍵VKを用いて、暗号化音楽情報EncCTに復号アルゴリズムD3を施して音楽情報CTを生成し、生成した音楽情報CTをデータ記憶部110へ書き込む。

ここで、暗号復号部109は、復号アルゴリズムE3として、DESを用いる。

また、暗号復号部109は、データ記憶部110から音楽情報CTを読み出し、前記時変鍵VKを用いて、音楽情報CTに暗号アルゴリズムE2を施して暗号化音楽情報EncCTを生成し、生成した暗号化音楽情報EncCTを暗号復号部210へ出力する。

ここで、暗号復号部109は、暗号アルゴリズムE2として、DESを用いる。

(11) データ記憶部110

データ記憶部110は、具体的には、半導体メモリから構成され、音楽情報CTを記憶する領域を備えている。

2.2 メモリカード20

メモリカード20は、共通鍵記憶部201、乱数種記憶部202、乱

数種更新部 203、乱数生成部 204、復号化部 205、分離部 206、相互認証部 207、時変鍵生成部 208、データ記憶部 209 及び暗号復号部 210 から構成されている。

(1) 共通鍵記憶部 201

5 共通鍵記憶部 201 は、具体的には、半導体メモリから構成され、56ビット長の共通鍵 UK を記憶している。共通鍵 UK は、メモリカード 20 の製造時に記録される。

共通鍵記憶部 201 は、外部から直接アクセスできる手段を有しておらず、プロテクトされている記憶手段である。

10 (2) 乱数種記憶部 202

乱数種記憶部 202 は、具体的には、半導体メモリから構成され、64ビット長の乱数種をあらかじめ記憶している。乱数種は、メモリカード 20 の製造時に記録される。

乱数種記憶部 202 は、外部から直接アクセスできる手段を有しておらず、プロテクトされている記憶手段である。

(3) 乱数生成部 204

乱数生成部 204 は、乱数種記憶部 202 から乱数種を読み出し、読み出した乱数種を用いて 64ビット長の乱数 R2 を生成し、生成した乱数 R2 を乱数種更新部 203 と、相互認証部 207 と、時変鍵生成部 208 とへ出力し、生成した乱数 R2 をリーダライタ装置 10 の相互認証部 107 と、時変鍵生成部 108 とへ出力する。

(4) 乱数種更新部 203

乱数種更新部 203 は、乱数生成部 204 から乱数 R2 を受け取り、受け取った乱数 R2 を新たな乱数種として乱数種記憶部 202 へ上書きする。

(5) 復号化部 205

復号化部 205 は、共通鍵記憶部 201 から共通鍵 UK を読み出し、暗号化部 105 から暗号化アクセス情報 R1 を受け取る。次に、読み出

した共通鍵UKを用いて、受け取った暗号化アクセス情報R1に、復号アルゴリズムD1を施して、乱数化アクセス情報を生成し、生成した乱数化アクセス情報を分離部206へ出力する。

5       ここで、復号化部205は、復号アルゴリズムD1として、DESを用いる。復号アルゴリズムD1は、暗号アルゴリズムE1により生成された暗号文を復号する。

#### (6) 分離部206

10       分離部206は、復号化部205から乱数化アクセス情報を受け取り、受け取った乱数化アクセス情報から、その上位32ビットのデータをアクセス情報として分離し、アクセス情報をデータ記憶部209へ出力する。

#### (7) 相互認証部207

15       相互認証部207は、共通鍵記憶部201から共通鍵UKを読み出し、暗号化アクセス情報R1を受け取り、受け取ったR1と共通鍵UKとを用いて、式4により、応答値V2を算出し、算出したV2をリーダライタ装置10の相互認証部107へ出力する。

$$(式4) \quad V2 = F1(R1, UK) = SHA(R1 + UK)$$

ここで、F1は、式1に示すF1と同じ関数であればよい。

20       また、相互認証部207は、乱数生成部204から乱数R2を受け取り、受け取った乱数R2と、前記共通鍵UKとを用いて、式5により、応答値V1'を算出する。

$$(式5) \quad V1' = F2(R2, UK) = SHA(R2 + UK)$$

ここで、F2は、式2に示すF2と同じ関数であればよい。

25       次に、相互認証部207は、相互認証部107からV1を受け取り、V1とV1'とが一致するか否かを判断し、一致しない場合には、リーダライタ装置10が不正な装置であると認定し、他の構成部に対して以降の動作の実行を禁止する。一致する場合には、相互認証部207は、リーダライタ装置10が正当な装置であると認定し、他の構成部に対し

て以降の動作の実行を許可する。

(8) 時変鍵生成部 208

時変鍵生成部 208 は、リーダライタ装置 10 が正当な装置であると認定され、動作の実行を許可される場合に、暗号化アクセス情報 R1 と乱数 R2 とを受け取り、R1 と R2 とから、式 6 を用いて時変鍵 VK を生成する

$$(式 6) \quad VK = F3(R1, R2) = SHA(R1 + R2)$$

ここで、F3 は、式 3 に示す関数 F3 と同じである。

次に、時変鍵生成部 208 は、生成した時変鍵 VK を暗号復号部 210 へ出力する。

(9) データ記憶部 209

データ記憶部 209 は、具体的には、半導体メモリから構成され、音楽情報 CT を記憶する領域を備えている。

(10) 暗号復号部 210

暗号復号部 210 は、時変鍵生成部 208 から時変鍵 VK を受け取る。

暗号復号部 210 は、暗号復号部 109 から暗号化音楽情報 EncCT を受け取り、前記時変鍵 VK を用いて、暗号化音楽情報 EncCT に復号アルゴリズム D2 を施して音楽情報 CT を生成し、生成した音楽情報 CT をデータ記憶部 209 の前記アクセス情報により示される領域へ書き込む。

ここで、暗号復号部 210 は、復号アルゴリズム D2 として、DES を用いる。復号アルゴリズム D2 は、暗号アルゴリズム E2 により生成された暗号文を復号する。

また、暗号復号部 210 は、データ記憶部 209 の前記アクセス情報により示される領域から音楽情報 CT を読み出し、前記時変鍵 VK を用いて、音楽情報 CT に暗号アルゴリズム E3 を施して暗号化音楽情報 EncCT を生成し、生成した暗号化音楽情報 EncCT を暗号復号部 109 へ出力する。

ここで、暗号復号部 210 は、暗号アルゴリズム E3 として、DES を用いる。復号アルゴリズム D3 は、暗号アルゴリズム E3 により生成された暗号文を復号する。

### 3. 認証通信システム 100 の動作

#### (1) 読み出し動作

認証通信システム 100 を構成するリーダライタ装置 10 及びメモリカード 20 の動作について、図 4～図 5 に示すフローチャートを用いて説明する。

なお、ここでは、リーダライタ装置 10 は、図 1 (b) に示すヘッドホンステレオのように、メモリカードに記憶されている情報を読み出す装置であると想定して説明する。

合成部 103 は、乱数種記憶部 102 から乱数種を読み出し、アクセス情報記憶部 101 からアクセス情報を読み出し、読み出した前記乱数種と読み出した前記アクセス情報とを合成して、乱数化アクセス情報を生成し (ステップ S101)、暗号化部は、共通鍵記憶部 104 から共通鍵を読み出し、読み出した前記共通鍵を用いて乱数化アクセス情報を暗号化して暗号化アクセス情報 R1 を生成し (ステップ S102)、相互認証部 107 は、 $V2' = F1(R1)$  を算出し (ステップ S103)、乱数種更新部 106 は、生成された乱数化アクセス情報を新たな乱数種として乱数種記憶部 102 に上書きする (ステップ S104)。

暗号化部 105 は、生成した暗号化アクセス情報 R1 をメモリカード 20 へ出力し、メモリカードの相互認証部 207 は、暗号化アクセス情報 R1 を受け取る (ステップ S105)。

相互認証部 207 は、 $V2 = F1(R1)$  を算出し (ステップ S106)、V2 をリーダライタ装置 10 の相互認証部 107 へ出力し、相互認証部 107 は、V2 を受け取る (ステップ S107)。

相互認証部 107 は、V2 と V2' とが一致するか否かを判断し、一致しない場合には (ステップ S108)、メモリカード 20 が不正な装置



であると認定し、以後の動作を中止する。

一致する場合には（ステップ S 1 0 8）、相互認証部 1 0 7 は、メモリカード 2 0 が正当な装置であると認定し、メモリカード 2 0 の乱数生成部 2 0 4 は、乱数種記憶部 2 0 2 から乱数種を読み出し、読み出した乱数種を用いて乱数 R 2 を生成し（ステップ S 1 0 9）、相互認証部 2 0 7 は、 $V 1' = F 2 (R 2)$  を算出し（ステップ S 1 1 0）、乱数種更新部 2 0 3 は、生成された乱数 R 2 を新たに乱数種として乱数種記憶部 2 0 2 に上書きする（ステップ S 1 1 1）。次に、乱数生成部 2 0 4 は、生成した乱数 R 2 をリーダライタ装置 1 0 の相互認証部 1 0 7 へ出力し、相互認証部 1 0 7 は、乱数 R 2 を受け取り（ステップ S 1 1 2）、相互認証部 1 0 7 は、 $V 1 = F 2 (R 2)$  を生成し（ステップ S 1 1 3）、生成した V 1 をメモリカード 2 0 の相互認証部 2 0 7 へ出力し、相互認証部 2 0 7 は、V 1 を受け取る（ステップ S 1 1 4）。

次に、相互認証部 2 0 7

相互認証部 2 0 7 は、V 1 と V 1' とが一致するか否かを判断し、一致しない場合には（ステップ S 1 1 5）、リーダライタ装置 1 0 が不正な装置であると認定し、以後の動作を中止する。

一致する場合には（ステップ S 1 1 5）、相互認証部 2 0 7 は、リーダライタ装置 1 0 が正当な装置であると認定し、リーダライタ装置 1 0 の時変鍵生成部 1 0 8 は、R 1 と R 2 とを用いて時変鍵 V K を生成する（ステップ S 1 2 1）。メモリカード 2 0 の復号化部 2 0 5 は、共通鍵記憶部 2 0 1 から共通鍵 U K を読み出し、読み出した共通鍵 U K を用いて R 1 を復号して乱数化アクセス情報を生成し（ステップ S 1 2 2）、分離部 2 0 6 は、乱数化アクセス情報からアクセス情報を分離し（ステップ S 1 2 3）、時変鍵生成部 2 0 8 は、R 1 と R 2 とを用いて時変鍵 V K を生成し（ステップ S 1 2 4）、暗号復号部 2 1 0 は、アクセス情報により示されるデータ記憶部 2 0 9 の領域から音楽情報 C T を読み出し（ステップ S 1 2 5）、暗号復号部 2 1 0 は、生成された時変鍵 V K を用いて読み出

した前記音楽情報 C T を暗号化して暗号化音楽情報 E n c C T を生成し  
(ステップ S 1 2 6)、生成した暗号化音楽情報 E n c C T をリーダライ  
タ装置 1 0 の暗号復号部 1 0 9 へ出力する (ステップ S 1 2 7)。

5 暗号復号部 1 0 9 は、時変鍵 V K を用いて暗号化音楽情報 E n c C T  
を復号して音楽情報 C T を生成してデータ記憶部 1 1 0 へ書き込み (ス  
テップ S 1 2 8)、入出力部 1 1 1 は、音楽情報 C T をデータ記憶部 1 1  
0 から読み出し、読み出した音楽情報 C T を音声信号に変換して出力す  
る (ステップ S 1 2 9)。

## (2) 書き込み動作

10 認証通信システム 1 0 0 を構成するリーダライタ装置 1 0 及びメモリ  
カード 2 0 の動作について、図 6 に示すフローチャートを用いて説明す  
る。

15 ここでは、リーダライタ装置 1 0 は、図 1 (a) に示すパーソナルコ  
ンピュータのように、メモリカードに情報を書き込む装置であると想定  
して説明する。また、読み出し動作と書き込み動作は類似しているので、  
相違点のみについて説明する。

図 4 ～図 5 のフローチャートのステップ S 1 2 5 ～S 1 2 9 を、図 6  
に示すステップに置き換えると認証通信システム 1 0 0 の書き込み動作  
となる。

20 暗号復号部 1 0 9 は、データ記憶部 1 1 0 から音楽情報 C T を読み出  
し (ステップ S 1 3 1)、時変鍵 V K を用いて読み出した音楽情報 C T を  
暗号化して暗号化音楽情報 C T を生成し (ステップ S 1 3 2)、生成した  
暗号化音楽情報 C T をメモリカード 2 0 の暗号復号部 2 1 0 へ出力し、  
暗号復号部 2 1 0 は、暗号化音楽情報 C T を受け取る (ステップ S 1 3  
25 3)。

暗号復号部 2 1 0 は、暗号化音楽情報 E n c C T を時変鍵 V K を用い  
て復号して音楽情報 C T を生成し (ステップ S 1 3 4)、生成した音楽情  
報 C T を前記アクセス情報で示されるデータ記憶部 2 0 9 内の領域に書

き込む（ステップ S 1 3 5）。

#### 4. まとめ

以上説明したように、相互認証と同時に、機密のデータを記録している機密データ記憶領域にアクセスするための情報を攪乱して転送するので、機密データ記憶領域にアクセスするための情報の機密性を高めることができる。

また、仮に機密データ記憶領域にアクセスするための情報が、不正になりすましにより、別の情報に改竄されて転送された場合であっても、相互認証が確立しないので、機密データ記憶領域にアクセスできないようにすることができる。

また、乱数の更新に機密データ記憶領域にアクセスするためのアクセス情報が関連していないので、乱数の周期性を高めることができる。

#### 5. 認証通信システム 1 0 0 a

認証通信システム 1 0 0 の変形例としての認証通信システム 1 0 0 a について説明する。

##### 5. 1 認証通信システム 1 0 0 a の構成

認証通信システム 1 0 0 a は、図 7 に示すように、リーダライタ装置 1 0 a とメモリカード 2 0 とから構成される。

メモリカード 2 0 は、図 2 に示すメモリカード 2 0 と同じであるので、ここでは、説明を省略する。

リーダライタ装置 1 0 a は、アクセス情報記憶部 1 0 1、乱数種記憶部 1 0 2、合成部 1 0 3、共通鍵記憶部 1 0 4、暗号化部 1 0 5、乱数種更新部 1 0 6、相互認証部 1 0 7、時変鍵生成部 1 0 8、暗号復号部 1 0 9、データ記憶部 1 1 0、入出力部 1 1 1 及び乱数生成部 1 1 2 から構成されている。

リーダライタ装置 1 0 との相違点を中心として、以下に説明する。その他の点については、リーダライタ装置 1 0 と同じであるので、説明を省略する。

(1) 乱数生成部 1 1 2

乱数生成部 1 1 2 は、乱数種記憶部 1 0 2 から乱数種を読み出し、読み出した乱数種を用いて 6 4 ビット長の乱数を生成し、生成した乱数を合成部 1 0 3 と乱数種更新部 1 0 6 とへ出力する。

5 (2) 乱数種更新部 1 0 6

乱数種更新部 1 0 6 は、乱数生成部 1 1 2 から乱数を受け取り、受け取った乱数を新たな乱数種として乱数種記憶部 1 0 2 へ上書きする。

(3) 合成部 1 0 3

10 合成部 1 0 3 は、乱数生成部 1 1 2 から乱数を受け取り、アクセス情報記憶部 1 0 1 からアクセス情報を読み出し、受け取った前記乱数と読み出した前記アクセス情報とを合成して、乱数化アクセス情報を生成する。

5. 2 認証通信システム 1 0 0 a の動作

15 認証通信システム 1 0 0 a の動作について、図 8 に示すフローチャートを用いて説明する。

乱数生成部 1 1 2 は、乱数種記憶部 1 0 2 から乱数種を読み出し（ステップ S 2 0 1）、読み出した乱数種を用いて 6 4 ビット長の乱数を生成し（ステップ S 2 0 2）、乱数種更新部 1 0 6 は、乱数生成部 1 1 2 から乱数を受け取り、受け取った乱数を新たな乱数種として乱数種記憶部 1 0 2 へ上書きする（ステップ S 2 0 3）。次に、合成部 1 0 3 は、乱数生成部 1 1 2 から乱数を受け取り、アクセス情報記憶部 1 0 1 からアクセス情報を読み出し、受け取った前記乱数と読み出した前記アクセス情報とを合成して、乱数化アクセス情報を生成する（ステップ S 2 0 4）。

25 次に、図 4 のステップ S 1 0 2 へ続く。以下は、認証通信システム 1 0 0 の動作と同じであるので、説明を省略する。

5. 3 まとめ

以上説明したように、乱数の更新に機密データ記憶領域にアクセスするためのアクセス情報が関連していないので、乱数の周期性を高めるこ

とができる。

## 6. 認証通信システム 100b

認証通信システム 100a の変形例としての認証通信システム 100b について説明する。

### 5 6. 1 認証通信システム 100b の構成

認証通信システム 100b は、図 9 に示すように、リーダライタ装置 10b とメモリカード 20b とから構成される。

#### (1) リーダライタ装置 10b の構成

10 リーダライタ装置 10b は、アクセス情報記憶部 101、乱数種記憶部 102、合成部 103、共通鍵記憶部 104、暗号化部 105、乱数種更新部 106、相互認証部 107、時変鍵生成部 108、データ記憶部 110、入出力部 111、乱数生成部 112、コンテンツ鍵生成部 113、暗号化部 114、コンテンツ付加情報記憶部 115、暗号復号部 116 及び暗号化部 117 から構成されている。

15 以下において、リーダライタ装置 10a との相違点を中心として説明する。その他の点については、リーダライタ装置 10a と同じであるので、説明を省略している。

#### (a) 入出力部 111

20 入出力部 111 は、利用者の操作によりコンテンツ付加情報の入力を受け付け、受け付けたコンテンツ付加情報をコンテンツ付加情報記憶部 115 に書き込む。

ここで、コンテンツ付加情報の一例は、コンテンツの再生回数、使用期間であり、コンテンツ付加情報は、8 ビット長である。

25 また、入出力部 111 は、利用者の操作によりコンテンツデータ CD を取得し、取得したコンテンツデータ CD をデータ記憶部 110 に書き込む。

ここで、コンテンツデータ CD は、一例として音楽コンテンツ情報である。

(b) 乱数生成部 1 1 2

乱数生成部 1 1 2 は、生成した乱数 R 3 をコンテンツ鍵生成部 1 1 3 へ出力する。

(c) コンテンツ鍵生成部 1 1 3

5        コンテンツ鍵生成部 1 1 3 は、コンテンツ付加情報記憶部 1 1 5 からコンテンツ付加情報を読み出し、乱数生成部 1 1 2 から乱数 R 3 を受け取り、乱数 R 3 と読み出したコンテンツ付加情報を用いて、式 7 により、コンテンツ鍵 C K を生成する。ここで、コンテンツ鍵 C K は、6 4 ビット長である。

10        (式 7)  $CK = F4(R3, \text{コンテンツ付加情報})$   
              = コンテンツ付加情報 (8 ビット長) + R 3 の下位 5 6 ビット

ここで、+ は、データとデータの結合を示す演算子である。

15        次に、コンテンツ鍵生成部 1 1 3 は、生成したコンテンツ鍵 C K を暗号化部 1 1 4 と、暗号化部 1 1 7 とへ出力する。

(d) 暗号化部 1 1 4

20        暗号化部 1 1 4 は、コンテンツ鍵生成部 1 1 3 からコンテンツ鍵 C K を受け取り、共通鍵記憶部 1 0 4 から共通鍵 U K を読み出し、読み出した共通鍵 U K を用いて、受け取ったコンテンツ鍵 C K に暗号化アルゴリズム E 4 を施して暗号化コンテンツ鍵 E n c C K を生成し、生成した暗号化コンテンツ鍵 E n c C K を暗号復号部 1 1 6 へ出力する。

ここで、暗号化部 1 1 4 は、暗号アルゴリズム E 4 として、D E S を用いる。(e) 暗号復号部 1 1 6

25        暗号復号部 1 1 6 は、暗号化部 1 1 4 から暗号化コンテンツ鍵 E n c C K を受け取り、受け取った暗号化コンテンツ鍵 E n c C K に、時変鍵 V K を用いて、暗号アルゴリズム E 2 を施して E n c (E n c C K) を生成し、生成した E n c (E n c C K) を暗号復号部 2 1 1 へ出力する。

ここで、暗号復号部 1 1 6 は、暗号アルゴリズム E 2 として、D E S



を用いる。

(f) 暗号化部 1 1 7

5 暗号化部 1 1 7 は、データ記憶部 1 1 0 からコンテンツデータ C D を読み出し、読み出したコンテンツデータ C D に、コンテンツ鍵 C K を用いて、暗号化アルゴリズム E 5 を施して暗号化コンテンツデータ E n c C D を生成する。次に、暗号化部 1 1 7 は、生成した暗号化コンテンツデータ E n c C D をデータ記憶部 2 1 3 へ出力する。

ここで、暗号化部 1 1 7 は、暗号アルゴリズム E 5 として、D E S を用いる。

10 (2) メモリカード 2 0 b の構成

メモリカード 2 0 b は、共通鍵記憶部 2 0 1、乱数種記憶部 2 0 2、乱数種更新部 2 0 3、乱数生成部 2 0 4、復号化部 2 0 5、分離部 2 0 6、相互認証部 2 0 7、時変鍵生成部 2 0 8、暗号復号部 2 1 1、鍵データ記憶部 2 1 2 及びデータ記憶部 2 1 3 から構成されている。

15 以下において、メモリカード 2 0 との相違点を中心として説明する。その他の点については、メモリカード 2 0 と同じであるので、説明を省略している。

(a) 時変鍵生成部 2 0 8

時変鍵生成部 2 0 8 は、時変鍵 V K を暗号復号部 2 1 1 へ出力する。

20 (b) 暗号復号部 2 1 1

暗号復号部 2 1 1 は、時変鍵生成部 2 0 8 から時変鍵 V K を受け取り、暗号復号部 1 1 6 から E n c (E n c C K) を受け取る。

次に、暗号復号部 2 1 1 は、時変鍵 V K を用いて E n c (E n c C K) に復号アルゴリズム D 2 を施して暗号化コンテンツ鍵 E n c C K を生成し、生成した暗号化コンテンツ鍵 E n c C K を前記アクセス情報により示される鍵データ記憶部 2 1 2 の領域に書き込む。

(c) 鍵データ記憶部 2 1 2

鍵データ記憶部 2 1 2 は、暗号化コンテンツ鍵 E n c C K を記憶する

領域を備える。

(d) データ記憶部 2 1 3

データ記憶部 2 1 3 は、暗号化コンテンツデータ  $E n c C D$  を受け取り、受け取った暗号化コンテンツデータ  $E n c C D$  を記憶する。

5 6. 2 認証通信システム 1 0 0 b の動作

認証通信システム 1 0 0 b の動作は、認証通信システム 1 0 0 a の動作に類似している。ここでは、認証通信システム 1 0 0 a との相違点についてのみ説明する。

10 認証通信システム 1 0 0 b の動作は、認証通信システム 1 0 0 a の動作を示すフローチャートのうち、ステップ S 1 2 1 以降を図 1 0 に示すフローチャートに置き換えたフローチャートにより示される。

15 コンテンツ鍵生成部 1 1 3 は、コンテンツ付加情報記憶部 1 1 5 からコンテンツ付加情報を読み出し (ステップ S 3 0 1)、乱数生成部 1 1 2 は、生成した乱数  $R 3$  をコンテンツ鍵生成部 1 1 3 へ出力し、コンテンツ鍵生成部 1 1 3 は、乱数生成部 1 1 2 から  $R 3$  を受け取り、 $R 3$  と読み出したコンテンツ付加情報を用いて、コンテンツ鍵  $C K$  を生成し、生成したコンテンツ鍵  $C K$  を暗号化部 1 1 4 と、暗号化部 1 1 7 とへ出力し (ステップ S 3 0 2)、暗号化部 1 1 4 は、コンテンツ鍵生成部 1 1 3 からコンテンツ鍵  $C K$  を受け取り、共通鍵記憶部 1 0 4 から共通鍵  $U K$  を読み出し、読み出した共通鍵  $U K$  を用いて、受け取ったコンテンツ鍵  $C K$  に暗号化アルゴリズム  $E 4$  を施して暗号化コンテンツ鍵  $E n c C K$  を生成し、生成した暗号化コンテンツ鍵  $E n c C K$  を暗号復号部 1 1 6 へ出力する (ステップ S 3 0 3)。次に、暗号復号部 1 1 6 は、暗号化コンテンツ鍵  $E n c C K$  を受け取り、受け取った暗号化コンテンツ鍵  $E n c C K$  に時変鍵  $V K$  を用いて暗号アルゴリズム  $E 2$  を施して  $E n c (E n c C K)$  を生成し (ステップ S 3 0 4)、暗号復号部 1 1 6 は、生成した  $E n c (E n c C K)$  を暗号復号部 2 1 1 へ出力し、暗号復号部 2 1 1 は、 $E n c (E n c C K)$  を受け取り (ステップ S 3 0 5)、暗号復号

部 2 1 1 は、E n c (E n c C K) に時変鍵 V K を用いて復号アルゴリズム D 2 を施して暗号化コンテンツ鍵 E n c C K を生成し、生成した暗号化コンテンツ鍵 E n c C K を前記アクセス情報により示される鍵データ記憶部 2 1 2 の領域に書き込む (ステップ S 3 0 6)。

- 5       暗号化部 1 1 7 は、データ記憶部 1 1 0 からコンテンツデータ C D を読み出し (ステップ S 3 0 7)、読み出したコンテンツデータ C D にコンテンツ鍵 C K を用いて暗号化アルゴリズム E 5 を施して暗号化コンテンツデータ E n c C D を生成する (ステップ S 3 0 8)。暗号化部 1 1 7 は、生成した暗号化コンテンツデータ E n c C D をデータ記憶部 2 1 3 へ出力し、データ記憶部 2 1 3 は、暗号化コンテンツデータ E n c C D を受け取り (ステップ S 3 0 9)、データ記憶部 2 1 3 は、受け取った暗号化コンテンツデータ E n c C D を記憶する (ステップ S 3 1 0)。
- 10

### 6. 3   まとめ

- 15       以上説明したように、認証通信システム 1 0 0 b において、コンテンツデータを暗号化するためのコンテンツ鍵を生成するのに、新たな乱数発生機構を必要とせず、アクセス情報の合成に用いる乱数発生機構と共有化できる。

### 7.   その他の変形例

- 20       なお、本発明を上記の実施の形態に基づいて説明してきたが、本発明は、上記の実施の形態に限定されないのはもちろんである。以下のような場合も本発明に含まれる。

- 25       (1) 上記の実施の形態において、デジタル著作物は、音楽の情報であるとしているが、小説や論文などの文字データ、コンピュータゲーム用のコンピュータプログラムソフトウェア、M P 3 などに代表される圧縮された音声データ、J P E G などの静止画像、M P E G などの動画像であるとしてもよい。

      また、リーダライタ装置は、パーソナルコンピュータに限定されず、上記の様々なデジタル著作物を販売したり配布したりする出力装置であ

るとしてもよい。また、リーダライタ装置は、ヘッドホンステレオに限定されず、デジタル著作物を再生する再生装置であるとしてもよい。例えば、コンピュータゲーム装置、帯型情報端末、専用装置、パーソナルコンピュータなどであるとしてもよい。また、リーダライタ装置は、上記出力装置と再生装置との両方を兼ね備えているとしてもよい。

(2) 上記の実施の形態において、暗号アルゴリズム及び復号アルゴリズムは、DESを用いるとしているが、他の暗号を用いるとしてもよい。

また、上記実施の形態において、SHAを用いるとしているが、他の一方向性関数を用いるとしてもよい。

共通鍵、時変鍵の鍵長は、56ビットであるとしているが、他の長さの鍵を用いるとしてもよい。

(3) 上記の実施の形態において、合成部103は、アクセス情報と、乱数種の下位32ビットとを結合して、64ビット長の乱数化アクセス情報を生成するとしているが、これに限定されない。次のようにしてもよい。

合成部103は、32ビットのアクセス情報と、乱数種の下位32ビットとを1ビットずつ交互に結合して、64ビット長の乱数化アクセス情報を生成してもよい。また、複数ビットずつ交互に結合してもよい。この場合、分離部206は、逆の操作を行うようにする。

(4) 上記の実施の形態において、メモ리카ード20の乱数生成部204は、乱数種記憶部202に記憶されている乱数種を用いて乱数R2を生成するとしているが、乱数生成部204は、乱数種を乱数R2として生成してもよい。

また、時変鍵生成部108、208は、R1及びR2を用いて時変鍵を生成するとしているが、応答値を用いるとしてもよい。また、共通鍵UKを絡ませてもよい。

(5) 認証通信システム100bにおいて、暗号化部117は、暗号化コンテンツデータEncCDをデータ記憶部213に書き込むとしてい

るが、暗号化コンテンツデータ E n c C D を機密データとして扱って、アクセス情報により示される領域に書き込むとしてもよい。

また、暗号化コンテンツ鍵 E n c C K を機密データとして扱わずに、データ記憶部 2 1 3 に書き込むとしてもよい。

5       また、暗号化部 1 1 4 及び暗号化部 1 1 7 のいずれか一方を無くし、残っている一方により共有化してもよい。

10       (6) 本発明は、上記に示す方法であるとしてもよい。また、これらの方法をコンピュータにより実現するコンピュータプログラムであるとしてもよいし、前記コンピュータプログラムからなるデジタル信号であるとしてもよい。

15       また、本発明は、前記コンピュータプログラム又は前記デジタル信号をコンピュータ読み取り可能な記録媒体、例えば、フロッピーディスク、ハードディスク、C D - R O M、M O、D V D、D V D - R O M、D V D - R A M、半導体メモリなど、に記録したものとしてもよい。また、これらの記録媒体に記録されている前記コンピュータプログラム又は前記デジタル信号であるとしてもよい。

      また、本発明は、前記コンピュータプログラム又は前記デジタル信号を、電気通信回線、無線又は有線通信回線、インターネットを代表とするネットワーク等を経由して伝送するものとしてもよい。

20       また、本発明は、マイクロプロセッサとメモリとを備えたコンピュータシステムであって、前記メモリは、上記コンピュータプログラムを記憶しており、前記マイクロプロセッサは、前記コンピュータプログラムに従って動作するとしてもよい。

25       また、前記プログラム又は前記デジタル信号を前記記録媒体に記録して移送することにより、又は前記プログラム又は前記デジタル信号を前記ネットワーク等を経由して移送することにより、独立した他のコンピュータシステムにより実施するとしてもよい。

      (4) 上記実施の形態及び上記変形例をそれぞれ組み合わせるとしても

よい。

#### 産業上の利用の可能性

- 5 デジタル著作物を出力する出力装置から半導体記録媒体へデジタル著作物を複製する場合において、出力装置と半導体記録媒体とが、相互に正当性を認証する場合に利用することができる。また、デジタル著作物の記録されている半導体記録媒体からデジタル著作物を読み出して再生する場合において、半導体記録媒体と再生装置との間で、各装置が、相互に正当性を認証する場合に利用することができる。



## 請 求 の 範 囲

1. デジタル情報を記憶する領域を有する記録媒体と、前記領域からデジタル情報を読み出し又は前記領域へデジタル情報を書き込むアクセス装置とから構成される認証通信システムであって、

前記アクセス装置から前記記録媒体へ、前記領域を示すアクセス情報を攪乱して生成した攪乱化アクセス情報を伝送することにより、前記アクセス装置がチャレンジレスポンス型の認証プロトコルによる前記記録媒体の正当性の認証を行う第1認証フェーズと、

前記記録媒体が前記アクセス装置の正当性の認証を行う第2認証フェーズと、

前記記録媒体と前記アクセス装置とがともに正当性を有すると認証された場合に、前記記録媒体は、伝送された攪乱化アクセス情報からアクセス情報を抽出し、前記アクセス装置は、抽出された前記アクセス情報により示される領域からデジタル情報を読み出し、又は前記アクセス情報により示される領域へデジタル情報を書き込む転送フェーズと

を含むことを特徴とする認証通信システム。

2. 前記第1認証フェーズにおいて、

前記アクセス装置は、

前記領域を示すアクセス情報を取得するアクセス情報取得部と、

乱数を取得する乱数取得部と、

取得した前記アクセス情報と、取得した乱数とを合成して乱数化アクセス情報を生成する生成部と、

生成した乱数化アクセス情報に暗号アルゴリズムを施して攪乱化アクセス情報を生成する暗号部とを含み、

前記記録媒体は、

生成された攪乱化アクセス情報から応答値を生成する応答値生成部とを含み、

前記アクセス装置は、

生成された前記応答値を用いて、前記記録媒体の正当性の認証を行う  
認証部を含む

ことを特徴とする請求の範囲 1 に記載の認証通信システム。

5 3. 前記転送フェーズにおいて、

前記記録媒体は、

生成された攪乱化アクセス情報に復号アルゴリズムを施して乱数化ア  
クセス情報を生成する復号部と、

10 伝送された乱数化アクセス情報からアクセス情報を分離する分離部と  
を含む

ことを特徴とする請求の範囲 2 に記載の認証通信システム。

4. 前記第 1 認証フェーズにおいて、

前記アクセス装置は、さらに、乱数種を記憶している乱数種記憶部を  
含み、

15 前記乱数取得部は、乱数種記憶部から乱数種を読み出すことにより、  
乱数を取得する

ことを特徴とする請求の範囲 3 に記載の認証通信システム。

5. 前記第 1 認証フェーズにおいて、

前記アクセス装置は、さらに、

20 前記攪乱化アクセス情報を乱数種として前記乱数種記憶部に上書きす  
る

ことを特徴とする請求の範囲 4 に記載の認証通信システム。

6. 前記第 1 認証フェーズにおいて、

25 前記アクセス装置は、さらに、乱数種を記憶している乱数種記憶部を  
含み、

前記乱数取得部は、乱数種記憶部から乱数種を読み出し、読み出した  
乱数種に基づいて乱数を生成することにより、乱数を取得する

ことを特徴とする請求の範囲 3 に記載の認証通信システム。

7. 前記第1認証フェーズにおいて、

前記アクセス装置は、さらに、

生成された前記乱数を乱数種として前記乱数種記憶部に上書きすること  
を特徴とする請求の範囲6に記載の認証通信システム。

5 8. 前記転送フェーズにおいて、

前記領域にデジタル情報を記録している記録媒体は、

前記アクセス情報により示される前記領域からデジタル情報を読み出し、読み出したデジタル情報に暗号アルゴリズムを施して暗号化デジタル情報を生成する暗号部を含み、

10 前記領域からデジタル情報を読み出す前記アクセス装置は、

生成された暗号化デジタル情報に復号アルゴリズムを施してデジタル情報を生成する復号部を含み、

前記復号アルゴリズムは、前記暗号アルゴリズムにより生成された暗号文を復号する

15 ことを特徴とする請求の範囲3に記載の認証通信システム。

9. 前記転送フェーズにおいて、

前記領域へデジタル情報を書き込む前記アクセス装置は、

デジタル情報を取得するデジタル情報取得部と、

取得したデジタル情報に暗号アルゴリズムを施して暗号化デジタル情報  
20 報を生成する暗号部を含み、

前記記録媒体は、

生成された前記暗号化デジタル情報に復号アルゴリズムを施してデジタル情報を生成し、前記アクセス情報により示される前記領域へデジタル情報を書き込む復号部を含み、

25 前記復号アルゴリズムは、前記暗号アルゴリズムにより生成された暗号文を復号する

ことを特徴とする請求の範囲3に記載の認証通信システム。

10. 前記転送フェーズにおいて、

前記領域へデジタル情報を書き込む前記アクセス装置は、

デジタル情報を取得するデジタル情報取得部と、

コンテンツ鍵を取得するコンテンツ鍵取得部と、

取得したコンテンツ鍵に第1暗号アルゴリズムを施して暗号化コンテンツ鍵を生成する第1暗号部と、

生成された前記暗号化コンテンツ鍵に第2暗号アルゴリズムを施して二重暗号化コンテンツ鍵を生成する第2暗号化部と、

前記コンテンツ鍵を用いて、取得した前記デジタル情報に第2暗号アルゴリズムを施して暗号化デジタル情報を生成する第3暗号部とを含み、

前記記録媒体は、

生成された前記二重暗号化コンテンツ鍵に第1復号アルゴリズムを施して暗号化コンテンツ鍵を生成し、前記アクセス情報により示される前記領域へ暗号化コンテンツ鍵を書き込む復号部を含み、

前記記録媒体は、さらに、生成された前記暗号化デジタル情報を記憶する領域を含む

ことを特徴とする請求の範囲3に記載の認証通信システム。

11. デジタル情報を記憶する領域を有する記録媒体と、前記領域からデジタル情報を読み出し又は前記領域へデジタル情報を書き込むアクセス装置とから構成される認証通信システムで用いられる認証通信方法であって、

前記アクセス装置から前記記録媒体へ、前記領域を示すアクセス情報を攪乱して生成した攪乱化アクセス情報を伝送することにより、前記アクセス装置がチャレンジレスポンス型の認証プロトコルによる前記記録媒体の正当性の認証を行う第1認証ステップと、

前記記録媒体が前記アクセス装置の正当性の認証を行う第2認証ステップと、

前記記録媒体と前記アクセス装置とがともに正当性を有すると認証された場合に、前記記録媒体は、伝送された攪乱化アクセス情報からアク

セス情報を抽出し、前記アクセス装置は、抽出された前記アクセス情報により示される領域からデジタル情報を読み出し、又は前記アクセス情報により示される領域へデジタル情報を書き込む転送ステップと

を含むことを特徴とする認証通信方法。

- 5 12. デジタル情報を記憶する領域を有する記録媒体と、前記領域からデジタル情報を読み出し又は前記領域へデジタル情報を書き込むアクセス装置とから構成され、前記記録媒体と前記アクセス装置との間において各機器の正当性の認証を行った後に、デジタル情報を転送する認証通信システムで用いられる認証通信プログラムを記録しているコンピュータ
- 10 読み取り可能な記録媒体であって、

前記認証通信プログラムは、

前記アクセス装置から前記記録媒体へ、前記領域を示すアクセス情報を攪乱して生成した攪乱化アクセス情報を伝送することにより、前記アクセス装置がチャレンジレスポンス型の認証プロトコルによる前記記録

15 媒体の正当性の認証を行う第1認証ステップと、

前記記録媒体が前記アクセス装置の正当性の認証を行う第2認証ステップと、

- 前記記録媒体と前記アクセス装置とがともに正当性を有すると認証された場合に、前記記録媒体は、伝送された攪乱化アクセス情報からアク
- 20 セス情報を抽出し、前記アクセス装置は、抽出された前記アクセス情報により示される領域からデジタル情報を読み出し、又は前記アクセス情報により示される領域へデジタル情報を書き込む転送ステップと
- を含むことを特徴とする記録媒体。

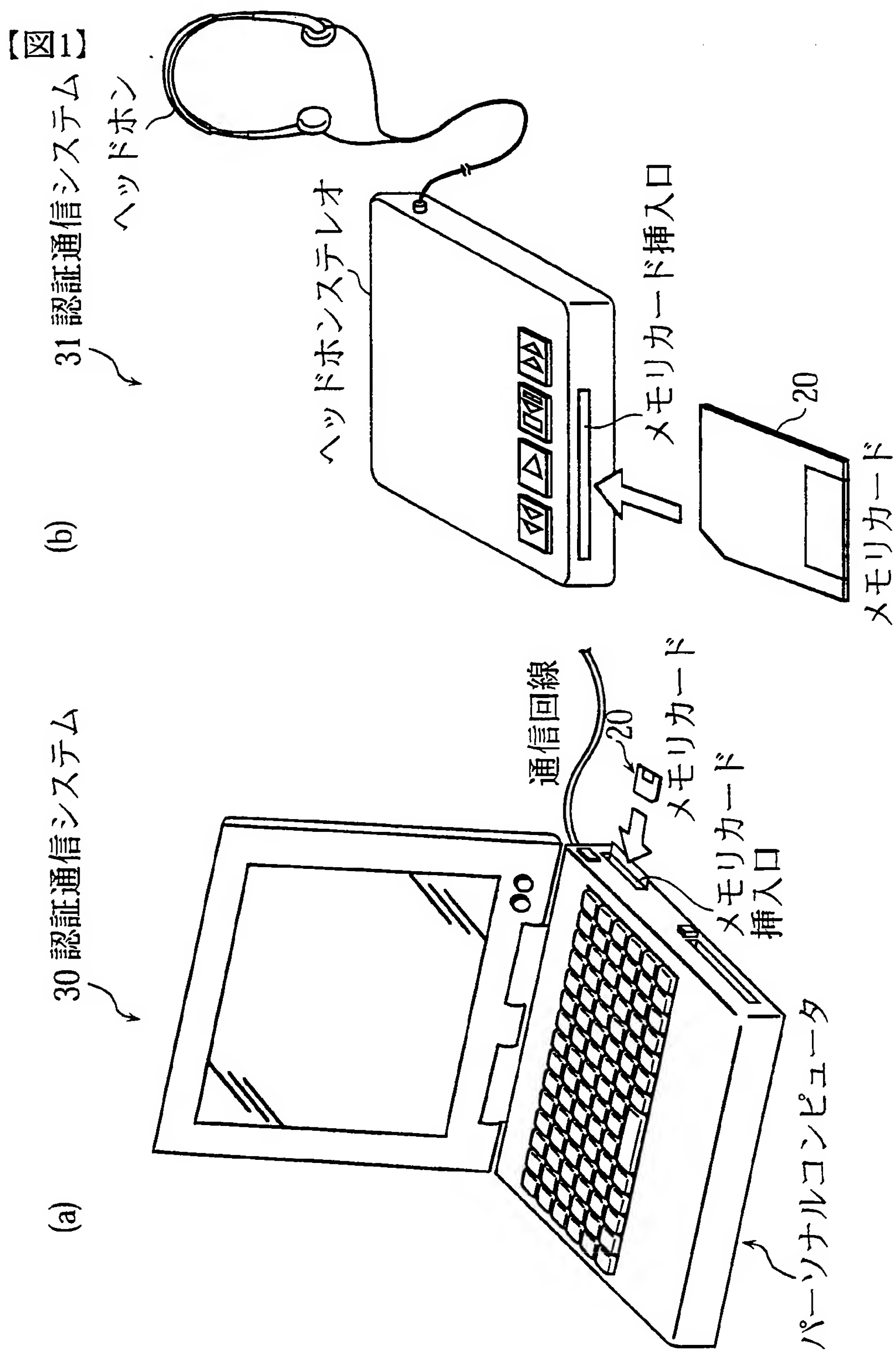
- 25 13. 請求の範囲1に記載の認証通信システムを構成するアクセス装置。

14. 請求の範囲2に記載の認証通信システムを構成するアクセス装置。

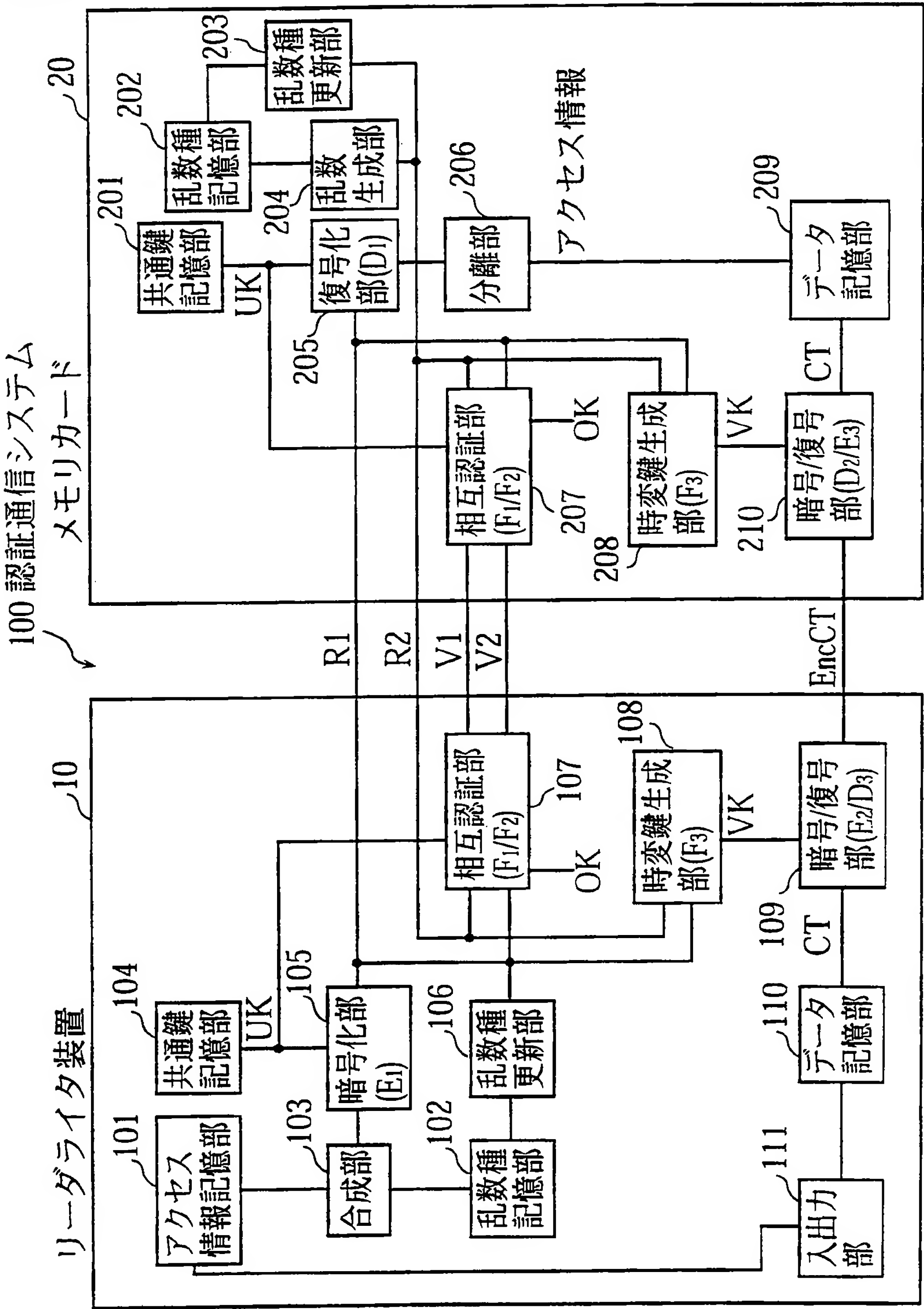
15. 請求の範囲 1 に記載の認証通信システムを構成する記録媒体。

16. 請求の範囲 3 に記載の認証通信システムを構成する記録媒体。

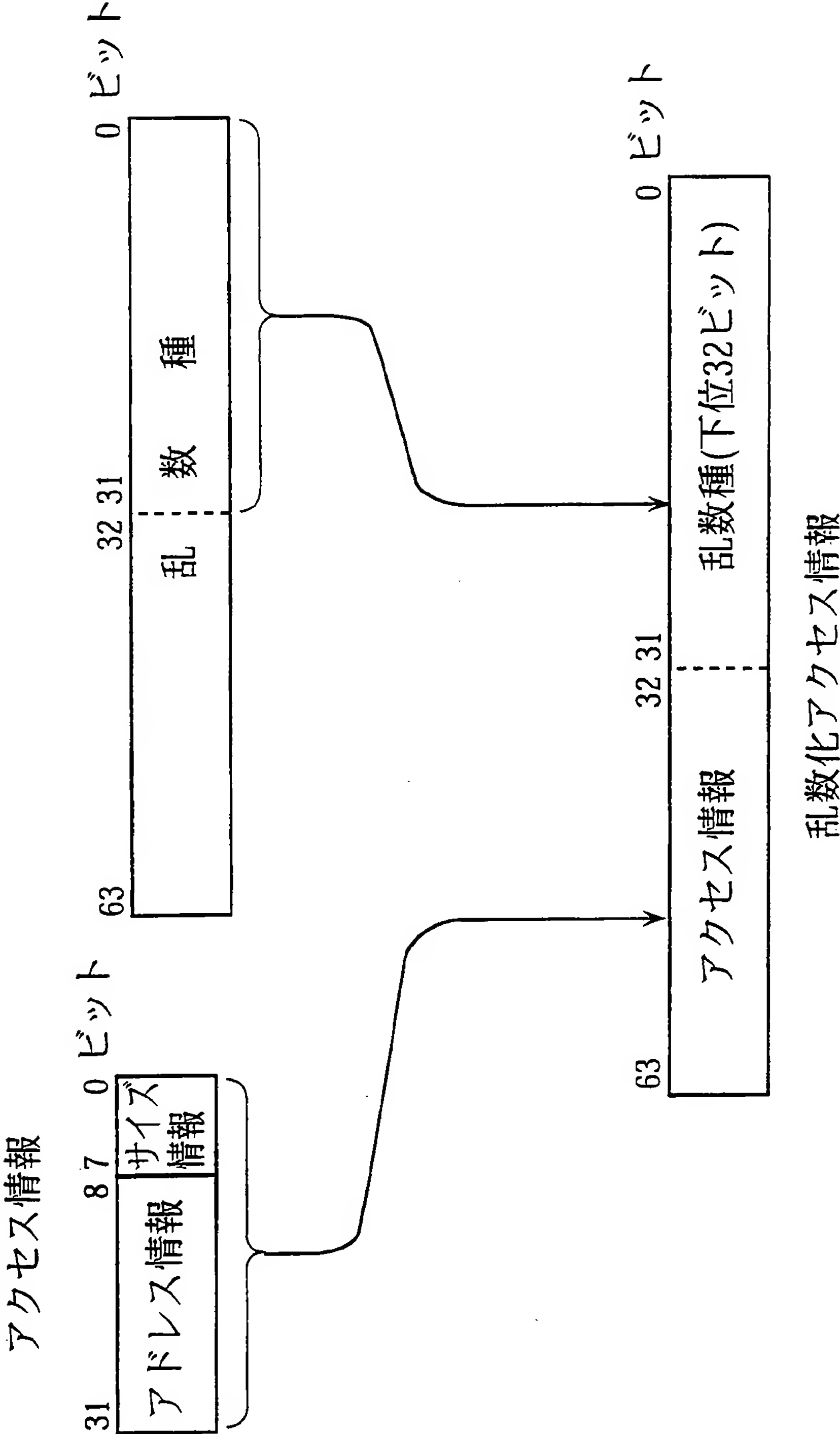




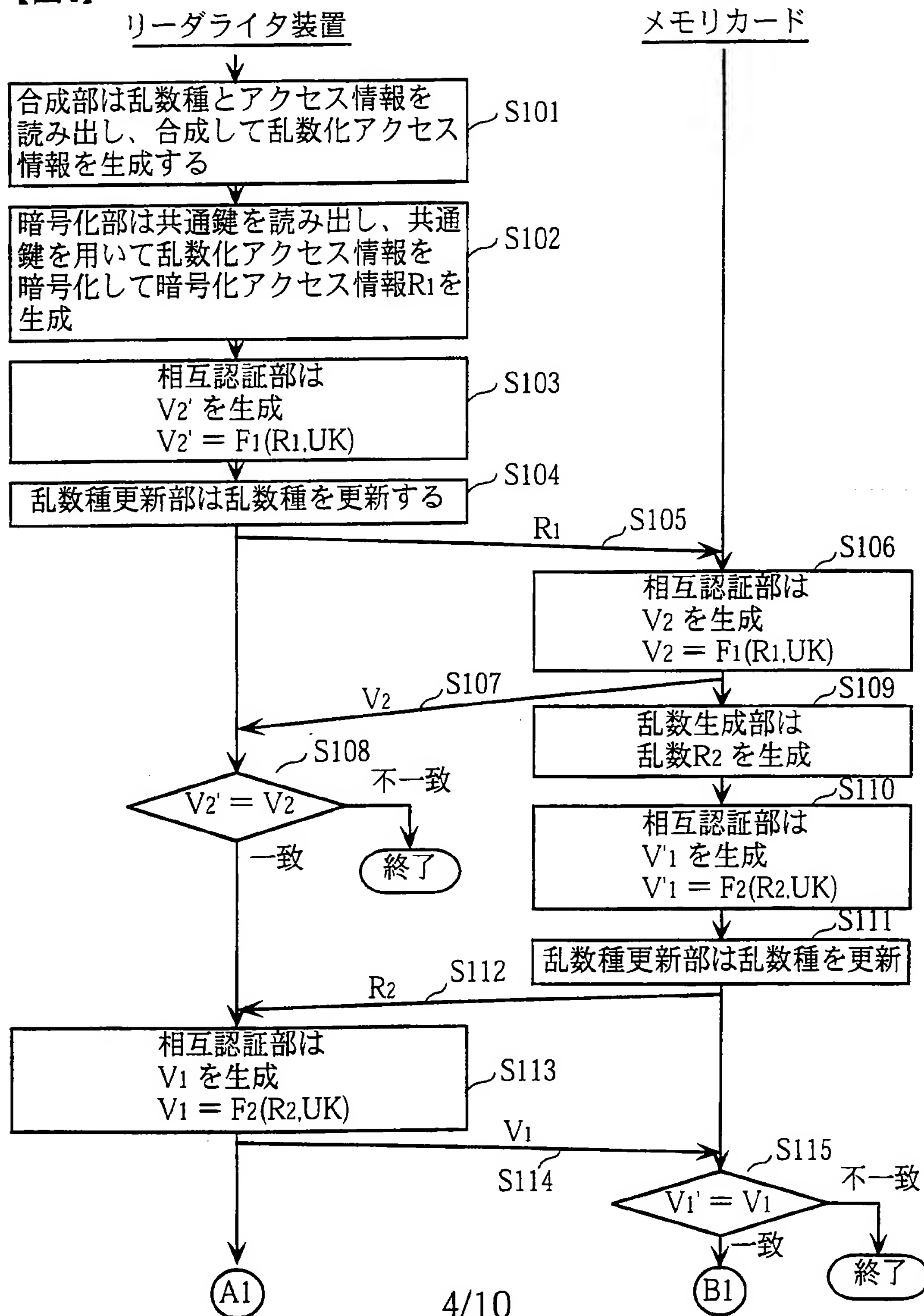
【図2】



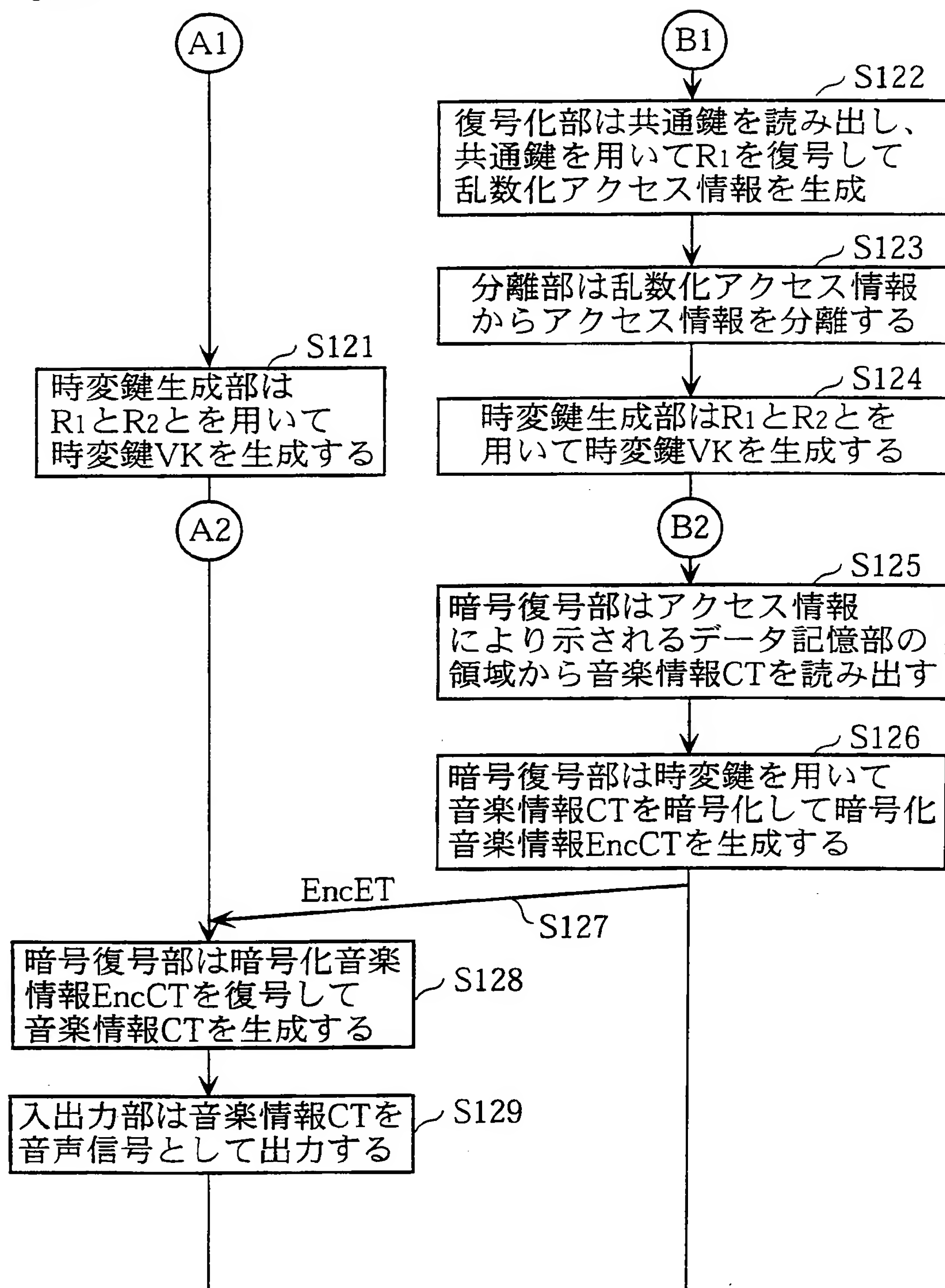
【図3】



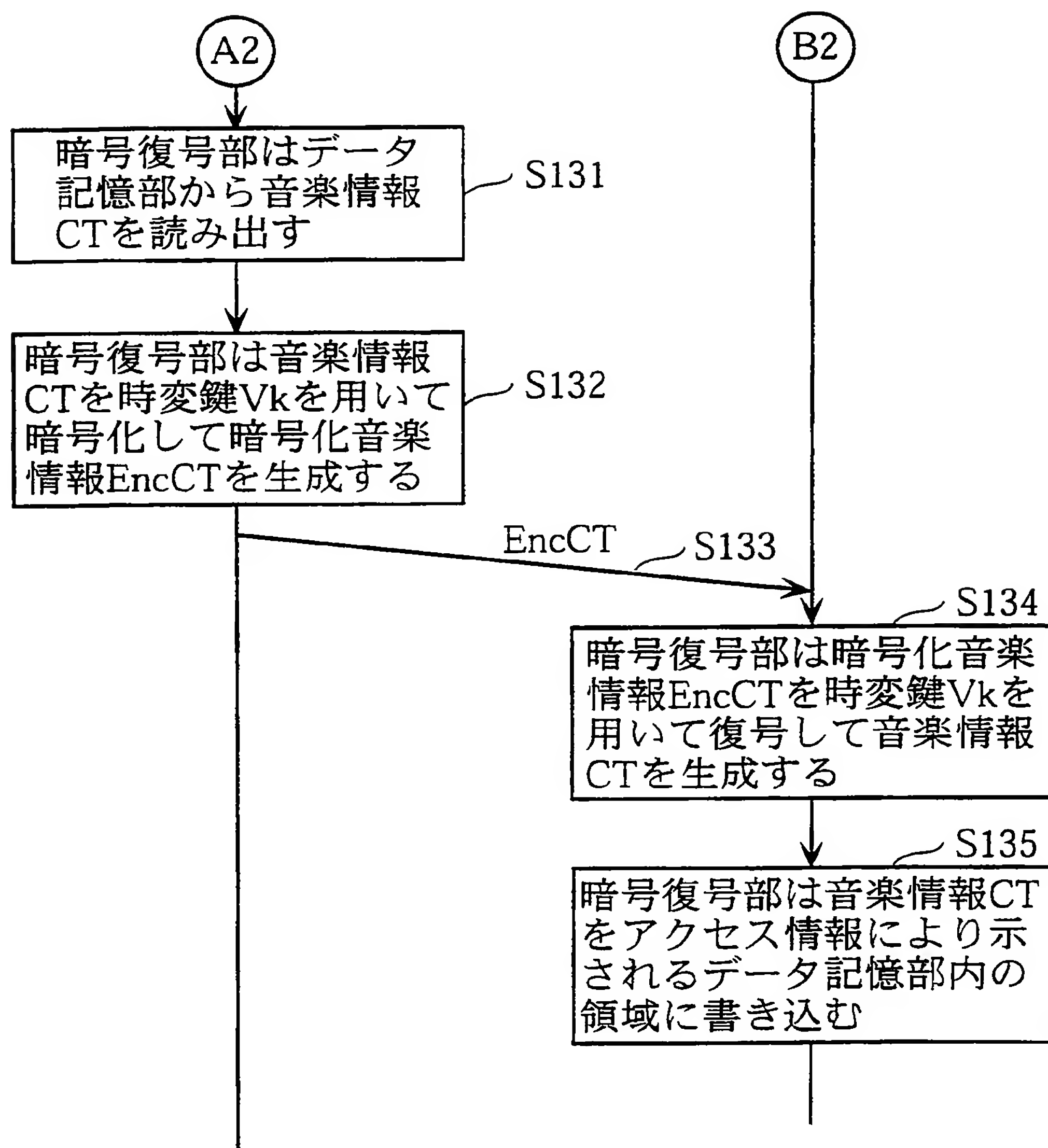
【図4】



【図5】



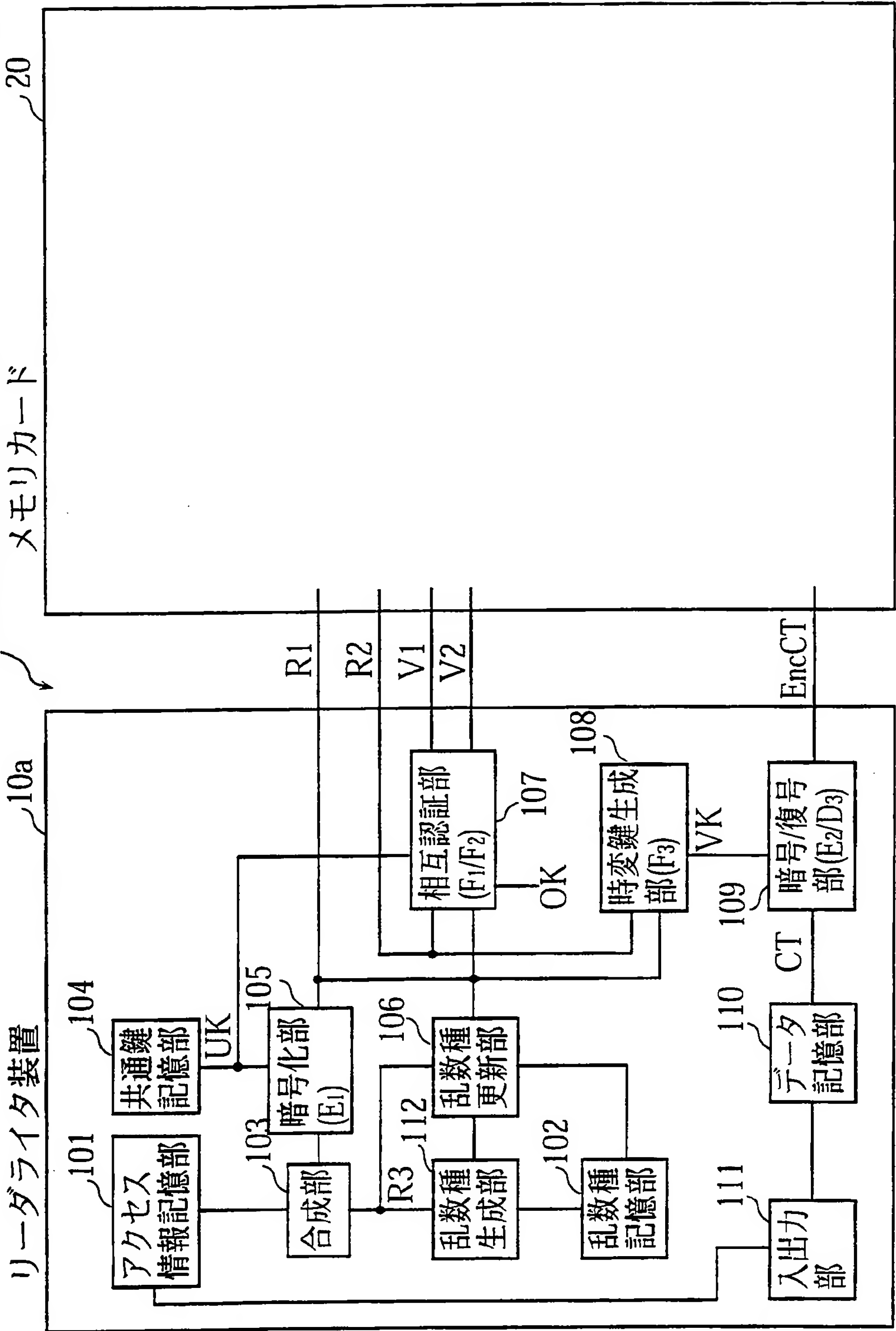
【図6】



【図7】

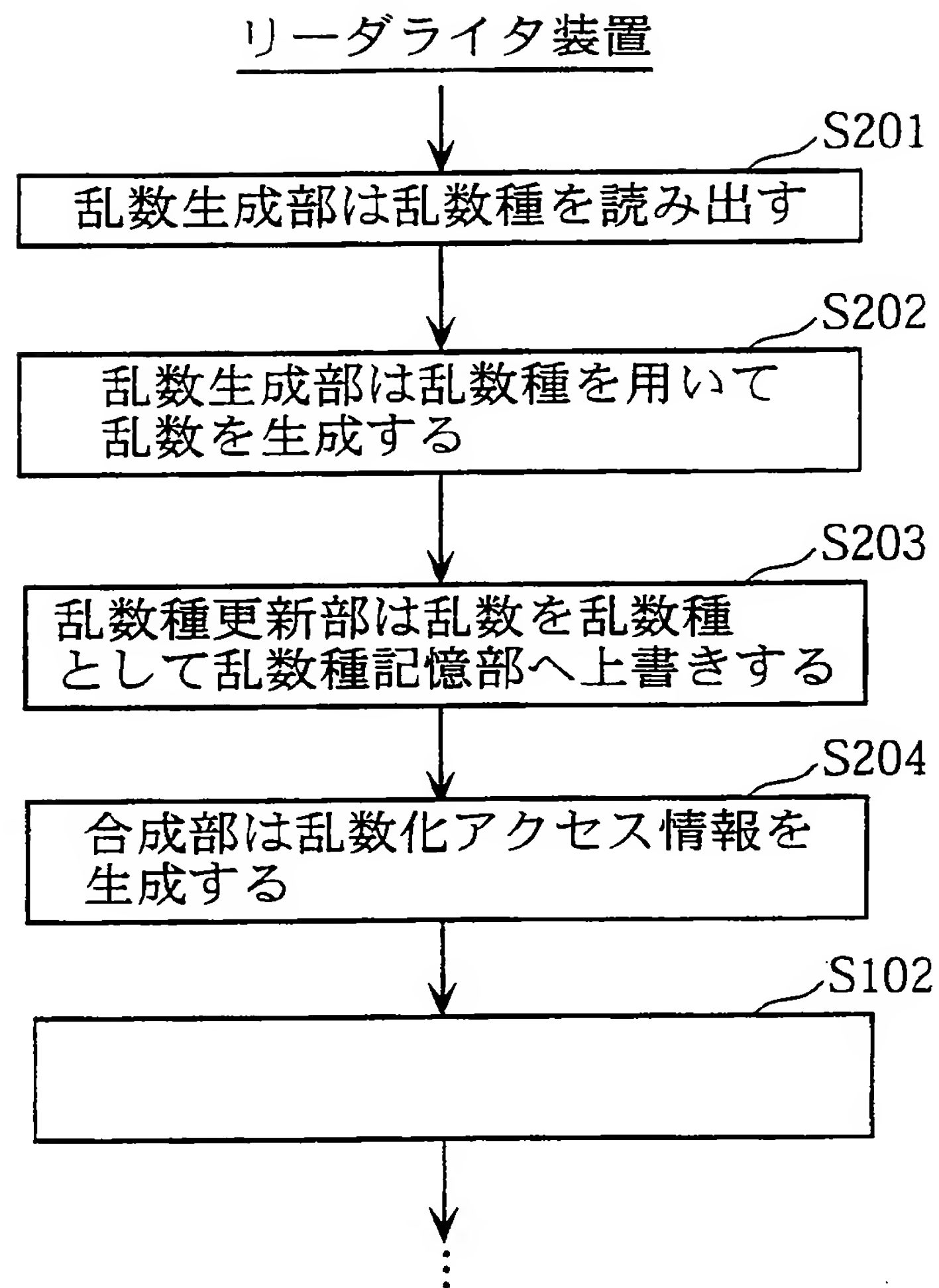
100a 認証通信システム

メモリカード





【図8】



【图9】

